Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996;	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information;	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277

To: The Commission

COMMENTS OF DOBSON COMMUNICATIONS CORPORATION

Dobson Communications Corporation ("Dobson")[1] hereby submits its comments in response to the Commission's notice of proposed rulemaking in the above-captioned proceeding.[2] Dobson submits that the Commission should not adopt any of the new Customer Propriety Network Information ("CPNI") security procedures that are under consideration in the *NPRM*. Implementation of these regulatory measures, in Dobson's view, will unnecessarily inconvenience consumers, unduly burden carriers and, most importantly, fail to address the

[1] Dobson is a provider of rural and suburban wireless communications services in 16 states, from Alaska to New York, with approximately 1.5 million customers and network operations covering a total population of over 11.9 million as of January 23, 2006. Dobson conducts its operations through two subsidiaries, Dobson Cellular Systems, Inc. and American Cellular Corporation, and offers services under the CELLULARONE® brand in all its markets except for those in western Oklahoma and the Texas panhandle, where Dobson uses the DOBSON CELLULAR SYSTEMS® service mark.

[2] *Implementation of the Telecommunications Act of 1996*, CC Docket No. 96-115, *Notice of Proposed Rulemaking*, FCC 06-10 (rel. Feb. 14, 2006) ("*NPRM*").

fraudulent conduct of the so-called "pretexters" or "social engineers."[3] The solution lies in the adoption and enforcement of laws that provide serious legal consequences to individuals that fraudulently obtain and sell phone records. In the event that some or all of the regulations under consideration in the *NPRM* are adopted, Dobson urges the Commission to include Tier II carriers within any exemption provided for smaller carriers.

I. Mandating Specific Carrier Safeguards Does Not Address The Root Problem.

Consumers are appropriately alarmed by the stealing and selling of cell phone records. The fact that data brokers can openly offer their "service" on the Internet for a small fee is equally intolerable. Professional pretexters are skilled and often armed with personal identifiers making them hard to detect and thwart.[4] The Commission must, however, recognize that carriers, like consumers, are victims in this situation. There is no evidence to suggest that carriers are freely disclosing subscriber information to anyone that asks. To the contrary, carriers like Dobson continue to invest significant resources to protect the privacy of subscribers from ever-changing security threats. Notwithstanding these procedures, the practice of acquiring fraudulently obtained cell phone records will continue – even if the regulatory requirements under consideration in this proceeding are adopted – so long as individuals that solicit and provide such "service" are not held accountable. The root problem that must be addressed, therefore, is individuals engaged in pretexting, not the security procedures employed by carriers. Congress is taking steps to resolve the problem now with the introduction of numerous bills that

---

[3] Dobson will use the term "pretexting" in its response because it has been accepted as a word that describes the practice in question. However, the terms "pretexting" or "social engineering" are too polite, and they mask the real nature of the practice, which is quite simply calling up a company and lying to them in order to pretend to be a customer or fellow employee who is entitled to the information sought.

[4] *See NPRM* at ¶ 15 (noting that data brokers are provided with biographical data on subscribers, such as a person's date of birth, mother's maiden name, or social security number, that is obtained through data mining or is provided by someone who knows the subscriber); *see also* Kevin D. Mitnick and William L. Simon, The Art of Deception – Controlling the Human Element of Security, (Wiley Publishing, Inc. 2002).

would outlaw the unauthorized access and sale of phone records.[5] If the problem continues after pretexting is made illegal, the Commission can then consider whether it would be appropriate to impose additional security regulations. Given the developments in Congress, it would be premature for the Commission to impose on the carriers at this time additional burdens that will reduce customer satisfaction and increase consumer costs.

II. Dobson's Current CPNI Security Procedures Are Adequate.

In the highly competitive cell phone industry, carriers must provide quality customer service to attract and retain subscribers. Carriers must protect subscriber information from unauthorized disclosure while also trying to not frustrate customers when they call to access or change their account information. Dobson fully realizes the value that customers place on the privacy of their call data and records, and Dobson takes its obligations to protect subscriber account information seriously. Dobson has thus installed a number of security measures to effect its compliance with Section 222, the Commission's rules, and to otherwise protect subscriber account information. While no amount of security can prevent all wrongdoers from gaining unauthorized access to customer information, Dobson's procedures appropriately balance the need to protect the customer's privacy interest against the need for customers to access their account information.

Dobson has trained its employees on the importance of safeguarding account information and implemented procedures to help insure that only the subscriber is given access to this information. Subscribers can obtain varying details about their account either by telephone

---

[5] *See* S. 2177; S. 2178; S. 2264; S. 2389; H.R. 4709; H.R. 4714; H.R. 4943, 109th Cong. (2006). H.R. 4709 passed in the House on April 25, 2006, by a vote of 405-0. Penalties for violations vary but certain proposals would make offenses criminal and punishable by fine and/or imprisonment for up to either 5, 10 or 20 years. *See* S. 2177; S. 2178; H.R. 4709; H.R. 4714. Another bill would instead create a private right of action with treble damages available and civil penalties ranging from $11,000 for a single violation to $11,000,000 for continuing violations. *See* S. 2389; *see also* S. 2264.

through customer service representatives ("CSRs") or an interactive voice recognition ("IVR") system, using the Internet to access Dobson's web self care facility, or through Dobson's retail stores. CSRs are provided with scripted verification procedures, and are trained on the proper way to conduct verification of customer identity. Subscribers must furnish verification information, and provide appropriate identification at retail stores, before obtaining account information. Employees are counseled and disciplined, as appropriate, for failing to follow established security procedures.

Employees are granted access only to the information systems that are necessary to perform their job function. However, most of Dobson's employees, including call center, sales, retail, and a limited number of corporate employees, are given access to some portions of subscriber account information because it is necessary to do their jobs. Agents at retail outlets not owned or controlled by Dobson do not have access to the billing system or information on calls made and received.

Subscribers are allowed to password protect their account, and if this is done, only someone who knows the password can pass the verification process and qualify to receive information from customer service over the telephone, from the web self care facility or by visiting a retail store. To establish or reset a password for Internet self care access, the subscriber must first provide verification information, after which a personal identification number ("PIN") is sent to the handset of the account holder via SMS text messaging.[6] Thus, only a person in possession of the handset can receive the new PIN. The PIN can be used to access the account to set or change the password. Dobson also allows passwords to be placed on the customer's account information. If the customer places a password on his or her account,

[6] *See* www.celloneusa.com (textual description displayed after accessing hyperlinks for setting and resetting passwords under "Manage My Account.").

anyone calling customer service must have the correct password in order to receive any information. Dobson recommends to subscribers that they set up passwords to their account if they suspect someone may attempt to access their information,[7] but only about 10% of the subscribers have taken advantage of password protection. Subscribers can block all web access to information so that neither they nor anyone else can obtain information over the Internet using Dobson's web self care facility. Copies of prior bills are not e-mailed or faxed, they are mailed to the address on the account.

III. Mandating Additional Security Measures Will Increase The Regulatory Burden For Wireless Carriers With Little Or No Benefit To Consumers.

Competition already gives carriers ample incentives to prevent unauthorized CPNI disclosure. Carriers like Dobson have thus implemented safeguards to protect CPNI with additional security options available to subscribers that want them. In the *NPRM*, the Commission is nonetheless considering imposing additional rules including, among other things, mandated customer-set passwords, audit trails, and a variety of notice requirements.[8] As noted herein, Dobson employs some of these safeguards already as an option to its subscribers, which allows the individual subscriber to balance the benefit of a particular security feature against the increased burden when accessing account information. Imposing across-the-board security measures for carriers and consumers prevents individuals from making their own cost-benefit analysis. Reviewing just a few of the regulatory measures addressed by the Commission in the *NPRM* demonstrates the problem:

---

[7] *Id.*

[8] These include: customer notification when an unauthorized disclosure of CPNI has occurred; advance notification to verify customer identity before disclosing CPNI; and post-notification in bill inserts or voicemail messages when a customer's CPNI records have been accessed. *See NPRM* at ¶¶ 15-18, 20-24, 27-30. Dobson submits that none of these measures should be adopted.

Mandated Passwords

Dobson already provides subscribers with the ability to password protect account information, but as noted above only 10% of the subscribers have set passwords.[9] Requiring Dobson to make all 1.5 million of its subscribers set passwords would be unduly burdensome and would be unnecessarily intrusive for those subscribers that do not want to set yet another password that must be remembered. Carriers should not be required to deny their customers service or account access unless the subscriber has set a password. Moreover, subscribers that forget their passwords will have to undergo certain procedures (through the carrier's website or through the customer service center) to reset them. Verification procedures for password resets will lead to potential pretexting attacks and customer service delays as subscribers wait to speak with a CSR that is conducting verification procedures.[10] None of this benefits consumers.

Audit Trails

A requirement that carriers maintain audit trails that record all instances of when a customer's records have been accessed, whether information was disclosed and to whom, would also be unduly burdensome. Modifications to billing and customer care software can be extremely costly. Accounts are accessed anytime a subscriber speaks with a CSR, interacts with the automated IVR system, or signs in to Dobson's web self care facility for routine inquiries relating to the account. Potentially then, almost every customer service related interaction could involve the access and/or use of CPNI and need to be tracked.

Dobson's billing system is programmed to track changes to account information, but not when it is accessed, used, or disclosed. For example, Dobson would have a record of password

---

[9] Dobson also provides subscribers with the ability to block all Internet access to account information, which is similar to the "no release" order proposal under consideration. *See NPRM* at ¶ 24.

[10] *Id.* at ¶ 8.

changes or changes to subscriber contact information, but not when the CSR or IVR informs the subscriber of his or her account balance, how many minutes have been used for the month, or the details of a particular call that resulted in a specific charge on a bill. Dobson's CSRs, the IVR system and the web self care facility combined handle about 35,000-45,000 calls or inquiries daily. Reprogramming to maintain audit trails for each of these calls would be a monumental and very expensive undertaking.

Notice

The notice proposals are unworkable. CPNI is never knowingly accessed or disclosed to persons who are not authorized to receive it. If CPNI is disclosed to an unauthorized person because the CSR using the scripted verification procedures has been successfully tricked by a pretexter, there is no awareness that anything unauthorized has occurred. While advance and post notification requirements are being considered to help identify successful pretexting, these notice requirements fail to take into account that many routine billing inquiries result in the access and disclosure of CPNI.[11] As recently noted at a Congressional hearing, "[w]ireless carriers collectively received hundreds of millions, if not billions, of customer inquiries in 2005."[12] Requiring notice in every instance could result in carriers inundating customers with often unwanted e-mails, text messages, or phone calls.

Dobson alone could generate at least 35,000-45,000 notices to its customers per day based on the average number of inquiries handled by its customer service, with most if not all involving accessing or disclosing CPNI. Numerous notices to customers would simply confuse and annoy customers with few notices actually helping to detect pretexting. Moreover,

---

[11] *NPRM* at ¶ 22; *see also* 47 U.S.C. § 222(h)(1) (defining CPNI to include information contained in bills pertaining to telephone exchange or toll service).

[12] *Phone Records for Sale: Why Aren't Phone Records Safe from Pretexting?: Hearing before the H. Comm. on Energy and Commerce*, 109th Cong. 71 (Feb. 1, 2006) (statement of the Hon. Steve Largent, Pres. and CEO, CTIA).

mandating such notification measures would burden the wireless industry with more notification requirements than currently provided for in financial transactions, where account holders do not receive notice every time they access their on-line brokerage account or engage in on-line banking. While aggregating notices in monthly billing statements may seem like a good alternative, billing systems and bills have limitations that may restrict the number of notifications (and the descriptions contained therein) in any given bill.[13]

Advance notification requirements (*i.e.*, pre-verification procedures) would prove equally unwieldy for customers and carriers. Imagine the customer frustration if, after going through the IVR system and waiting to speak with the CSR to discuss a charge on a bill, the CSR tells the customer that he or she must first call the registered telephone number to verify customer identification. Perhaps the customer is using the registered number to call the CSR or calling from work and is not near the registered number to verify.

Encryption

The issue in this proceeding is the theft of calling records. Pretexters who steal CPNI are seeking the records of a particular customer to see where the customer is, who the customer is calling, and who is calling the customer. They do that by tricking carrier employees into thinking that they are the customer or a fellow employee. CPNI that is in a customer bill or displayed on a CSR's screen can obviously not be encrypted. Encryption would be a counter-measure against thefts of large amounts of data, but there is no evidence that CPNI has been stolen in bulk. Without a specific target, the call detail records of an entire set of customers for a day or week has no value to a pretexter. Obviously, a file that contains a useful set of data for identity thieves, for example, the name, social security number and credit card number of a group

[13] *See* Comments of Dobson, CC Docket No. 98-170 (filed June 24, 2005).

of customers, should be protected. That sort of data is not at issue in this proceeding, and the obligations of carriers to protect such data are no different from the obligations of businesses generally.

IV. Any Exemptions Should Extend To Tier II Carriers.

Should the Commission decide to impose new regulations, any exemptions adopted should be applied to Tier II carriers. Notwithstanding its current status as a Tier II carrier and the 7th largest wireless carrier in the United States, Dobson is dwarfed by the Tier I carriers. For purposes of comparison, Dobson serves approximately 1.5 million subscribers versus Cingular with 49.1 million and Verizon Wireless with 43.8 million.[14] Dobson thus must spread the costs of regulatory obligations over a much smaller customer base, resulting in Dobson's subscribers, who are located in the rural and suburban areas that Dobson primarily serves, bearing a higher percentage of the cost than the customers of Tier I carriers. Accordingly, Dobson and other Tier II carriers would more appropriately be deemed a small carrier for exemption purposes.

[14] *See Annual Report and Analysis of Competitive Market Conditions With Respect to Commercial Mobile Services*, WT Docket No. 05-71, *Tenth Report*, 20 FCC Rcd 15908, Appendix A, Table 4 (2005).

CONCLUSION

For the reasons stated above, Dobson urges the Commission not to adopt the additional CPNI security procedures that are under review in this proceeding.

Respectfully submitted,

DOBSON COMMUNICATIONS CORPORATION

By: /s/ Ronald L. Ripley

Ronald L. Ripley, Esq.
Senior Vice President & General Counsel
Dobson Communications Corporation
14201 Wireless Way
Oklahoma City, OK 73134
(405) 529-8500

April 28, 2006